801

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/781,311	02/18/2004	Vincent Dupaquis	ATM-244	4864

3897 7590 07/13/2007

SCHNECK & SCHNECK
P.O. BOX 2-E
SAN JOSE, CA 95109-0005

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
07/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/781,311	DUPAQUIS ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :5/21/04; 5/27/04; 8/27/04; 4/22/05; 4/27/05.

DETAILED ACTION

1. Claims 1-13 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). ***Information Disclosure Statement***

3. The information disclosure statements (IDS) submitted on 21 May 2004, 27 May 2004, 27 August 2004, 22 April 2005, and 27 April 2007are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statements.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. The term "approximate" in claims 1-13 is a relative term which renders the claim indefinite. The term "approximate" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. See MPEP § 2173.05(b).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barrett's modular reduction method in view of U.S. Patent Application No. 2003/0044014 A1 to Liardet

et al., hereinafter Liardet.

8. As per claim 1, Barrett's method involves precomputing and storing in memory a constant U representing a bit-scaled reciprocal of a modulus M and estimating an approximate quotient q for a number X to be reduced modulo M, wherein said estimating is executed upon X in a computation unit by a multiplication by said constant U and by bit shifts of X and a shift of said multiplication as shown by page 5, lines 8-13 of Applicant's specification. This is further supported by pages 603-605 of **The Handbook of Applied Cryptography**, which was submitted in the IDS of 27 April 2005. Barrett's method also calculating a remainder R' = X - q'M in said computation unit, said remainder being larger than said modulus M but congruent to X modulo M, as shown by Equation 1, of Section 2.2 on page 385 of **The Chinese Remainder Theorem and its Application in a high-speed RSA crypto Chip**, which was submitted by the Applicant in the IDS of 27 August 2004.

9. Barrett's method does not disclose generating in a random number generator a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient q' = q – E.

10. Liardet teaches modifying an intermediary result with a random quantity, carrying out the calculation and restoring the expected result at the end of the modular reduction (paragraphs 0033-0035, 0041).

11. It would have been obvious to one of ordinary skill in the at the time the invention was made to generate, in a random number generator, a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient q' = q – E, since Liardet

states at paragraph 0031 that adding a random intermediary value to a calculation provides protection against attacks by differential power analysis.

12. Regarding claims 2 and 10, Barrett's method teaches wherein precomputing said constant U is performed according to the equation $U = [b^{2n+1}/M]$, where $b = 2^w$, with w being the word size of the computation unit in bits, as show via evidentiary evidence of Sections 14.42 and 14.44 of **The Handbook of Applied Cryptography**. This is further supported equation 4 on page 386 of **The Chinese Remainder Theorem and its Application in a high-speed RSA crypto Chip**.

13. With regards to claims 3 and 11, Barrett's method teaches wherein estimating the approximate quotient q is performed by the computation unit according to the equation $q = [([X/b^n] \cdot U) / b^{n+2}]$, as show by evidentiary evidence of Sections 14.42 and 14.44 of **The Handbook of Applied Cryptography**.

14. Concerning claims 4 and 12, Barrett's method teaches wherein a supplemental subtraction by one is included in the quotient estimation, as show via evidentiary evidence of Section 2.2 of **The Chinese Remainder Theorem and its Application in a high-speed RSA crypto Chip**.

15. Regarding claim 5, Liardet teaches wherein the modular reduction of X is part of a computer hardware-implemented cryptography program (paragraphs 0002, 0041).

16. Regarding claim 6, Liardet does not teach wherein an alternate calculation pathway is provided wherein generating and applying an error value to the approximate quotient may be selectively omitted. The Examiner notes that if the applying the error value to the approximate quotient is omitted, claim 1 recites Barrett's method.

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a selection process for including the error value, since it would have only required routine skill in the art to include the alternate path of omitting the error value. See MPEP § 2144.04; see *In re Kuhle*, 526, F.2d 553, 188 USPQ 7 (CCPA 1975).

18. Regarding claims 7 and 13, Barrett's method teaches wherein the random number generator has a specified error limit of one-half word, whereby $0 <= E < (2^{w/2} - 1)$, as show by evidentiary evidence of Section 14.43 of **The Handbook of Applied Cryptography**.

19. Claims 8-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior Art in view of Barrett's Method, and further in view of Liardet.

20. As per claim 8, Applicant's admitted prior art discloses computational hardware for executing a cryptographically secure modular reduction method, the hardware comprising a computation unit adapted to perform word-wide multiply and accumulate steps on operands retrieved from a memory and carry terms from a set of registers and an operations sequencer comprising logic circuitry for controlling the computation unit as discussed from page 3, line 23 to page 4, line 9. Barrett's method, as disclosed by page 5, lines 8-13 of Applicant's

specification is a method to carry out a modular reduction of a number X with respect to a modulus M that involves at least an estimation of an approximate quotient q from a pre-stored constant U representing a bit-scaled reciprocal of the modulus and calculation of a remainder value R' = X - q'M.

21. As established by the Applicant the prior art does not show the above systems with a random number generator for generating a random error value E; and calculating a randomization of said the approximate quotient with said random error value E to obtain a randomized quotient q' = q - E.

22. Liardet teaches modifying an intermediary result with a random quantity, carrying out the calculation and restoring the expected result at the end of the modular reduction (paragraphs 0033-0035, 0041).

23. It would have been obvious to one of ordinary skill in the at the time the invention was made to generate, in a random number generator, a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient q' = q – E, since Liardet states at paragraph 0031 that adding a random intermediary value to a calculation provides protection against attacks by differential power analysis.

24. Regarding claim 9, Applicant's admitted prior art teaches operation parameter registers accessible by said operations sequencer, said registers containing any one or more of (a) pointers for locating operands within said memory, (b) information about lengths of operands, (c) carry injection control information for carry term registers, and (d) destination address information for intermediate results of operation steps (page 3, line 35 to page 4, line 2).

Double Patenting

25. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

26. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

27. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

28. Claims 1-7 are provisionally rejected on the ground of nonstatutory double patenting over claims 1-6 of copending Application No. 11/203,939. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

29. The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows (similarities shown using **bold**):

Claim 1, Instant Application	Claim 1, Application #11/203,939
A cryptographically secure, computer hardware-implemented modular reduction method, comprising: **precomputing and storing in memory a constant U representing a bit-scaled reciprocal of a modulus M;** **estimating an approximate quotient q for a number X to be reduced modulo M, wherein said estimating is executed upon X in a computation unit by a multiplication by said constant U and by bit shifts of X and a shift of said multiplication;** **generating in a random number generator a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient** q' = q – E (); and **calculating a remainder** R' = X - q'M **in said computation unit, said remainder being larger than said modulus M but congruent to X modulo M**.	**A cryptographically secure, computer hardware-implemented modular reduction method** in the binary finite field GF(2^n), comprising: **precomputing and storing in memory** a polynomial **constant u(x) representing a bit-scaled reciprocal of a** polynomial **modulus m(x);** **estimating an approximate quotient q for a number p(x) to be reduced modulo m(x), wherein said estimating is executed upon p(x) in a computation unit by a** polynomial multiplication over GF(2^n) **by said constant u(x) and by bit shifts;** **generating in a random number generator a random** polynomial **error value E(x) and applying said** polynomial **error value to said approximate polynomial quotient to obtain a randomized quotient** q'(x) = q(x) + E(x);. and **calculating a remainder** r'(x) = p(x) + q'x · m(x) **in said computation unit, said remainder r'(x) being of high degree than said modulus m(x) but congruent to p(x) modulo m(x)** and where the degree of p(x) is less than or equal to 2k+1.

30. Furthermore, there is no apparent reason why applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

31. Claims 8-13 are provisionally rejected on the ground of nonstatutory double patenting over claims 7-11 of copending Application No. 11/203,939. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

32. The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows (similarities shown using **bold**):

Claim 8, Instant Application	Claim 7, Application #11/203,939
Computational hardware for executing a cryptographically secure modular reduction method, the hardware comprising: **a computation unit adapted to perform word-wide multiply and accumulate steps on operands retrieved from a memory and carry terms from a set of registers;** **a random number generator for generating a random error value E;** **an operations sequencer comprising logic circuitry for controlling the computation unit and random number generator in accord with program instructions so as to carry out a modular reduction of a number X with respect to a modulus M that involves at least an estimation of an approximate quotient q from a pre-stored constant U representing a bit-scaled reciprocal of the modulus, a randomization of said the approximate**	**Computational hardware for executing a cryptographically secure** polynomial **modular reduction method** over a binary finite field GF(2^n), the hardware comprising: **a computation unit adapted to perform word-wide** finite-field **multiply and accumulate steps on** polynomial **operands retrieved from a memory and** polynomial coefficient intermediate **results from a set of working registers;** **a random number generator for generating a random** polynomial **error value E(x);** **an operations sequencer comprising logic circuitry for controlling the computation unit and random number generator in accord with program instructions so as to carry out a** polynomial **modular reduction of a number p(x) with respect to a modulus m(x)** over a binary finite field GF(2^n) **that involves at least an**

quotient with said random error value E to obtain a randomized quotient q' = q - E, **and a calculation of a remainder value** R' = X - q'M.	**estimation of a** polynomial **quotient q(x) from a pre-stored** polynomial **constant u(x) representing a bit-scaled reciprocal of the modulus, a randomization of said the approximate** polynomial **quotient with said random** polynomial **error value E(x) to obtain a randomized polynomial quotient** q'(x) = q(x) + E(x), **and a calculation of a polynomial remainder value** r'(x) = p(x) + q'x · m(x).

33. Furthermore, there is no apparent reason why applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Conclusion

34. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

35. The following patents are cited to further show the state of the art with respect to modular reduction, such as:

United States Patent No. 5,724,279 to Benaloh et al., which is cited to show a computer-implemented method for performing modular reduction.

United States Patent No. 7,164,765 B2 to Nishioka et al., which is cited to show modular reduction used for generating keys for public key encryption.

36. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

37. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

38. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf